(U) The Crypto-Mathematics Institute Has the Formula

FROM: Joe McCloskey
CMI President
Run Date: 06/24/2005

(U//FOUO) The Crypto-Mathematics Institute (CMI) is the oldest of the Learned Organizations at NSA. It was established by Lieutenant General John A. Samford, Director, NSA, in a memorandum dated October 1957. The CMI has been an integral part of the mathematics community at NSA ever since its inception.

(U//FOUO) The purpose of the Institute is to promote those aspects of mathematics which pertain to cryptology and to provide a focal point for the NSA mathematics community in fields of common interest. Its membership is open to anyone with an interest in crypto-mathematics.

(U//FOUO) CMI sponsors a variety of social and scholarly events, often in conjunction with an Agency office or the Professional Health Program (PHP). Recently, on June 2-3, 2005, CMI and CES co-sponsored **MATHFEST**. As part of MATHFEST, Professor Dan Boneh of Stanford gave an invited talk on bilinear maps in cryptography. Professor Boneh heads the applied crypto group at the Computer Science Department at Stanford University. Dr. Boneh's research focuses on applications of cryptography to computer security. He is the author of over 70 publications in the field. Dr. Boneh's work includes e-mail security, security for handheld devices and web servers, digital copyright protection, and cryptanalysis. He is a recipient of the Packard Award, the Alfred P. Sloan Award, and the Terman Award.

(U//FOUO) This year's MATHFEST program also included eight classified talks by members of the community on a wide range of topics of current interest, including presentations on cryptanalysis, statistics, applied mathematics, and computer science.

(U//FOUO) The Institute bestows a variety of honors at the annual banquet: essay contest prizes, Distinguished Memberships, Distinguished Service, CMI President's Award, and the CMI Teaching Award.

- The **CMI Essay Contest** was established in 1959 to recognize outstanding written contributions to the fields of mathematics and cryptology.
- The **Distiguished Members** form the CMI Hall of Fame, drawn from retirees in the extended classified mathematics community.
- The **Distinguished Service Award** is made to individuals who have made significant contributions to the health of the community.
- Since 1978, the **CMI President's Award** (or mathematician of the year) has recognized Agency personnel who are making important contributions to the mission of the cryptologic community through the

SERIES:
(U) Learned Orgs '05

development and application of the science of mathematical cryptology.

- The **CMI Teaching Award** was established in 1997 to honor important teaching contributions to the mathematics community.

(U//FOUO) These awards are given at the annual **CMI banquet.** This year's banquet was held on Friday, June 3 at Snyder's Willow Grove. In addition to the annual awards presentations, this year's banquet included a special tribute to Dr. Richard Leibler, whose contributions to mathematical practice and theory were crucial to America's national security. His technical knowledge and managerial abilities helped transform IDA into an institution that kept NSA in the forefront of mathematical and cryprologic capability in the 1960s and 1970s. Working together with Dr. Solomon Kullback, Dr. Leibler devised a new method of measuring similarity between populations; this statistical function bears their name and is still used widely on a diverse set of different statistical applications.

(U//FOUO) A complete listing of CMI officers and activities appears on the internal website, [redacted] (or "go cmi").
